SOLUTION BRIEF

Comprehensive Solutions for PCI DSS 4.0 Compliance

One integrated platform for Proactive Security and Proactive Threat Detection for Enhanced Payment Protection

Problem

In today's evolving threat landscape, protecting cardholder data requires more than just checking compliance boxes. The stark reality is that cybercriminals are leveraging increasingly sophisticated tactics, with phishing attacks surging since the introduction of AI tools like ChatGPT. This dramatic shift has created new challenges for security professionals, particularly in securing email communications and collaboration platforms where sensitive payment data often flows freely. The latest PCI-DSS 4.0 framework acknowledges these emerging threats, introducing enhanced requirements for email security and digital collaboration that demand a more comprehensive approach to data protection. The new framework mandates specific controls, from anti-phishing mechanisms to mandatory multi-factor authentication for all cardholder data environment access, but implementing these controls effectively requires a deeper understanding of how modern attacks operate – especially considering who is being targeted, humans. Security professionals must now navigate a complex intersection of compliance requirements and real-world threats. The path forward requires a balanced strategy that combines technical controls with human awareness.

$500,000 in fines faced by organizations per incident for PCI DSS non-compliance[1]

67% of businesses that experienced a data breach reported it involved payment card data[2]

60% of small businesses close within six months of a data breach due to financial and reputational damage, which can stem from non-compliance with PCI DSS standards[3]

Key Benefits

- **Achieve PCI DSS 4.0 Compliance with Confidence:** Simplify compliance efforts with tools designed to meet strict requirements for email authentication, secure communication, and data protection.
- **Secure Sensitive Cardholder Data:** Protect against email-borne threats, including phishing and spoofing, while ensuring encrypted transmission of sensitive payment data.
- **Enhance Visibility and Control:** Gain actionable insights into email traffic and potential threats, empowering admins to make informed security and compliance decisions.

1 PCI Security Standards Council
2 Verizon 2023 Data Breach Investigations Report
3 National Cyber Security Alliance

Solution

Mimecast's human risk management platform delivers comprehensive protection for cardholder data, while streamlining compliance efforts and addressing critical PCI DSS 4.0 requirements. The platform's multi-layered approach starts with:

- DMARC Analyzer, providing visibility into email authentication and preventing domain spoofing that could compromise payment data.
- Advanced Email Security employs AI-powered detection to block sophisticated threats targeting cardholder information, while ensuring compliance with PCI DSS requirements for secure transmission over open networks.
- Aware transforms how organizations protect cardholder data across digital collaboration platforms, employing advanced pattern matching and machine learning algorithms to identify payment information. The solution's continuous monitoring detects exposed credit card numbers in real-time, while automated governance controls enable immediate response actions when violations occur.
- Mimecast Engage directly addresses the human element of payment security through awareness training – especially when 95% of data breaches involve human error.
- Secure Messaging ensures communications remain protected through strong encryption and secure portal delivery, meeting PCI DSS Requirements for data protection.

Through automated security measures, intuitive user experiences, and continuous protection, organizations can confidently handle sensitive payment information while meeting their evolving PCI DSS 4.0 obligations.

> *"With Mimecast, we've been able to stop domain spoofing attacks to take back control of the Bradley brand and protect our employees, customers and supply chain—all while keeping our in-house resources focused on strategic business projects. Mimecast is truly committed to our success, and it shows."*
>
> **Dave Leannah**
> Vice President of IT, Bradley Corp

Use Cases

Domain Spoofing

Problem: A global financial services firm discovered multiple instances of their domain being spoofed to target their customers and supply chain with fraudulent emails.

Solution: The organization implemented DMARC Analyzer with a strategic approach, starting with monitoring mode to gather baseline data. The platform's identified legitimate versus unauthorized email sources, and through gradual enforcement level increases and continuous monitoring of legitimate email delivery.

Protecting Cardholder Data in Collaboration Platforms

Problem: A retail organization using collaboration platforms discovered employees inadvertently sharing payment card information in messages and files.

Solution: The company deployed Aware's Spotlight, implementing real-time content scanning across all collaboration channels. Advanced pattern matching and machine learning algorithms identified cardholder data, while automated governance controls enabled immediate response actions.

Credential Phishing Attacks

Problem: A banking institution faced sophisticated phishing attacks targeting employee credential using AI-generated content and legitimate service abuse. Several successful attacks had led to compromised accounts and potential data breaches.

Solution: The organization implemented Mimecast email security utilizing AI-powered threat detection to identify sophisticated phishing attempts. Mimecast Engage provided targeted training, creating a multi-layered defense against credential theft.

About Mimecast

Mimecast is a leading AI-powered, API-enabled connected Human Risk Management platform, purpose-built to protect organizations from the spectrum of cyber threats. Integrating cutting-edge technology with human-centric pathways, our platform enhances visibility and provides strategic insight that enables decisive action and empowers businesses to protect their collaborative environments, safeguard their critical data and actively engage employees in reducing risk and enhancing productivity. More than 42,000 businesses worldwide trust Mimecast to help them keep ahead of the ever-evolving threat landscape. From insider risk to external threats, with Mimecast customers get more. More visibility. More insight. More agility. More security.